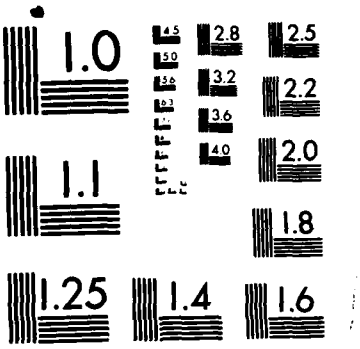
AD-A161 883 PRELIMINARY HAZARD ANALYSIS FOR SELF-CONTAINED NAVIGATION SYSTEM(U) LEAR SIEGLER INC GRAND RAPIDS MI INSTRUMENT DIV J T REEVES 04 OCT 85 MISC-2037 1/1

UNCLASSIFIED F09603-85-C-1224 F/G 17/7 NL



PRELIMINARY HAZARD ANALYSIS

FOR

SELF-CONTAINED NAVIGATION SYSTEM

REPORT NO. MISC-2037

4 OCTOBER 1985

Contract No. F09603-85-C-1224

LEAR SIEGLER, INC.
INSTRUMENT DIVISION

PRELIMINARY HAZARD ANALYSIS

FOR

SELF-CONTAINED NAVIGATION SYSTEM

REPORT NO. MISC-2037

4 OCTOBER 1985

Contract No. F09603-85-C-1224

Data Item 0103

Prepared by: J. T. Reeves

J. T. Reeves

Approved by: H. Stark

H. Stark

TABLE OF CONTENTS

Title	Page No.
SUMMARY	3
GENERAL	4
PURPOSE	4
SCOPE	4
APPLICABLE DOCUMENTS	4
SYSTEM DESCRIPTION	5
GENERAL DESCRIPTION	5
MAJOR COMPONENTS	8
ICDS	8
INS	8
DVS	8
SYSTEM FUNCTIONS	8
MAJOR FUNCTIONS	8
SECONDARY FUNCTIONS	8
A KITS	9
SAFETY CRITERIA	10
SYSTEM SAFETY PRECEDENCE	10
HAZARD LEVEL CATEGORIES	10
HAZARD SEVERITY	10
HAZARD PROBABILITY	11
HAZARD ANALYSIS MATRIX SHEETS	11

APPENDIX I
HAZARD ANALYSIS MATRIX SHEETS

SUMMARY

The Preliminary Hazard Analysis (PHA) has been prepared IAW CDRL 0103 for the C-130 Self-Contained Navigation System (SCNS).

The PHA has been applied to the installation of the SCNS Equipment IAW 84-MMSRE-004-C-130-SCNS Rev.G and 84-MMSRE-009-C-130 Rev.G.

No confirmed Category I or II hazards have been found. Item 10 of the Appendix is a speculative Category II hazard and should not occur in the final design.

1.0 GENERAL - This document constitutes the Preliminary Hazard Analysis (PHA) for the C-130 Self-Contained Navigation System (SCNS) installation. It provides an initial risk assessment of the SCNS installation.

1.1 PURPOSE - IAW MIL-STD-882A, "the purpose of the PHA is to identify safety critical areas, evaluate hazards, and identify the safety design criteria to be used". The items covered in this analysis are to be used during the design phase and trade-off study period to prevent unsafe concepts, designs, or oversights that could lead to incorporation of hazards in the hardware, the system operation, handling, and maintenance.

1.2 SCOPE - The scope of this analysis for Data Item 0103 is limited to the SCNS installation task "A-kit" components (viz. wiring harness, brackets, racks, control panels, relay boxes, circuit breakers), "B-kit" components (viz. ICDUs, BICU, DVS, INU), and the physical interfaces with existing equipment (viz. CADC or Sensors, Radar, Air Data Sensors). These items will be analyzed in respect to safe installation, safe hardware, and safe usage (viz. installation, removal, in-place test, and handling).

2.0 APPLICABLE DOCUMENTS

MIL-STD-882A	System Safety Program Requirements (paragraph 5.5.1.1) (Preliminary Hazard Analysis)
DI-H-7048	System Safety Hazard Analysis Report (paragraph 10.2.1)
DH1-6	System Safety Design Handbook
SOW 84-MMSRE-004-C-130-SCNS Rev.G	C-130 Modification Self-Contained Navigation System (SCNS), Statement of Work for
84-MMSRE-009-C-130 Rev.G	Self-Contained Navigation System (SCNS), Integration, Fabrication and Installation and Test of, C-130 Aircraft

3.0 SYSTEM DESCRIPTION

3.1 GENERAL DESCRIPTION - The SCNS is comprised of a Doppler Velocity Sensor (DVS), Inertial Navigation System (INS), Integration Computation and Display System (ICDS), and the associated installation Group A kit to provide doppler aided INS navigation, INS only, Doppler only and TAS/HDG navigation modes, and control of the various C-130 communication/navigation (comm/nav) systems. The SCNS ICDS consists of three Integrated Control Display Units (ICDU) and one Bus Integration Computer Unit (BICU) for all C-130 aircraft except that the HC-130H will have an additional ICDU for the radio operation. A block diagram is shown in figure 1.

In conjunction with the SCNS installation, the following systems/components will be removed from the various C-130 configurations.

AN/APN-147 Doppler
AN/ASN-35 Doppler Computer
ARN-131 Omega
AN/ASN-24 or PINS (C-130E AWADS only)

Radio controls for

AN/ARC-164 UHF
AN/ARC-186 VHF
AN/ARC-190 HF
AN/ARN-118 TACAN
AN/ARN-127 VOR/ILS
USAF Standard VOR/ILS

The communication and navigation radio control functions will be assumed by the ICDUs.

3.2 MAJOR COMPONENTS - A list of major components is provided in table I.

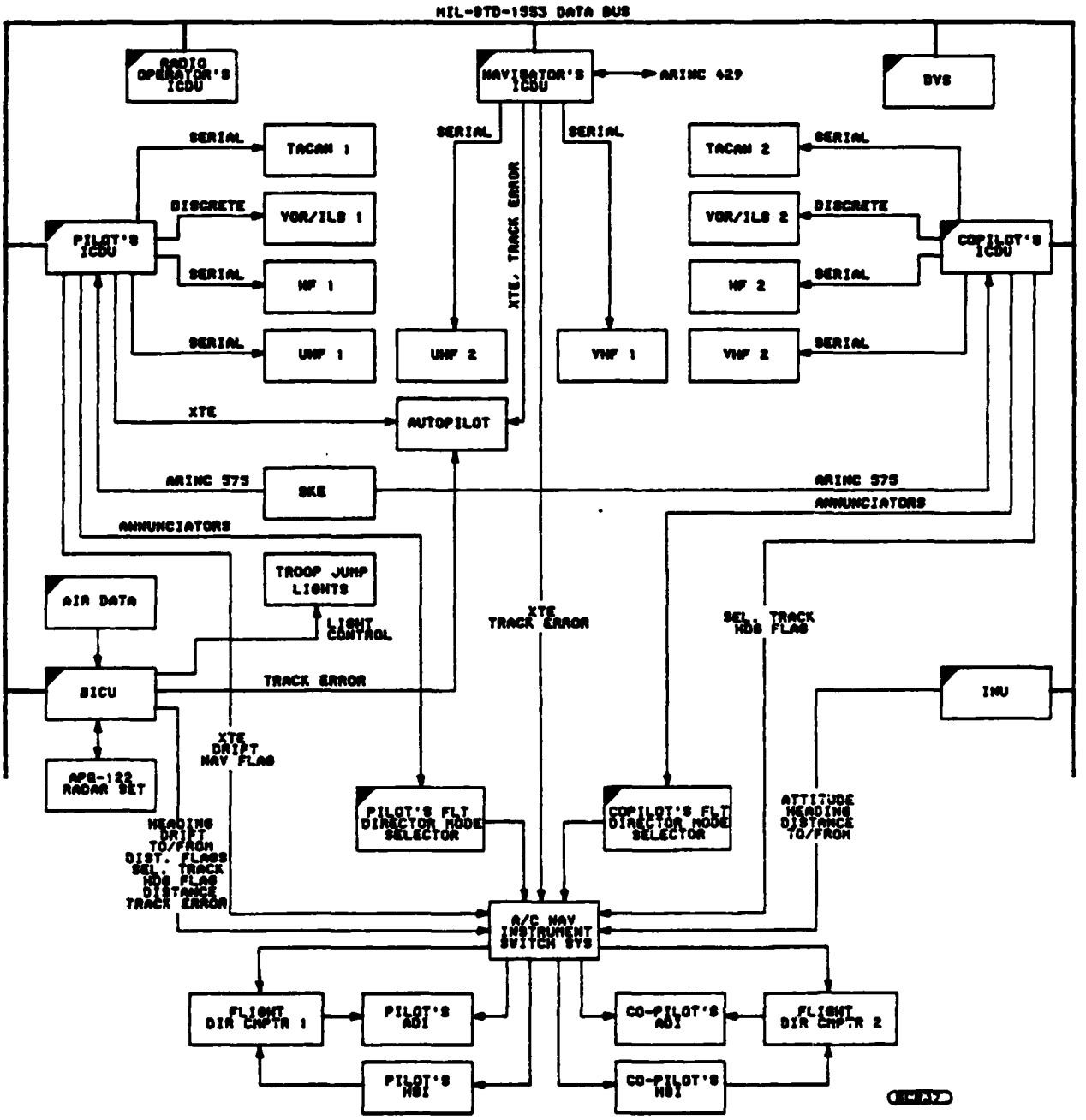


Figure 1. SCNS Block Diagram

Table I. Major Component List

MODEL NO.	GROUP		DESCRIPTION	LOCATION
	A	B		
LSI-2580F		√	Integrated Control Display Unit	Left side forward on center console for pilot. Right side forward for co-pilot. Nav panel for navigator. Radio operator's panel for HC-130.
LSI-2905A		√	Bus Interface Computer Unit	New equipment rack.
LSI-2905B		√	Bus Interface Computer Unit with Added Radar Interface Card (AWADS)	New equipment rack.
LSI-2590A APN-218		√	Doppler Velocity Sensor	Belly of aircraft
SNU 84-1		GFE	Inertial Navigation Sensor	Aircraft floor below new equipment rack
Dwg No's. TBD	√		Electrical A-Kit	Several variations
Dwg No's. TBD	√		Mechanical A-Kit	Several variations
-	√		Flight Director Mode Select panel modifications	
-	√		SCNS Control Panel	

3.2 ICDS - The ICDS consists of two major components: the Integrated Control Display Unit (ICDU) and the Bus Integration Computer Unit (BICU). All aircraft configurations utilize fully interchangeable ICDUs: pilot's, co-pilot's, navigator's and radio operator's (HC-130H). Jumper wires in the aircraft installation indicate its particular station location to each ICDU. One basic BICU design is utilized in all SCNS configurations. Jumper wires in the aircraft installation for the BICU indicate in which aircraft model the BICU is installed.

3.2.2 INS - The Inertial Navigation System (INS) consists of three major components: the Inertial Navigation Unit (INU), the INU mount, and the SCNS battery subsystem. The SCNS INU conforms to requirements of the F^3 SNU 84-1 specification.

3.2.3 DVS - The Doppler Velocity Sensor (DVS) consists of the APN-218 Airforce Standard Doppler. The DVS provides basic navigation inputs for SCNS independent doppler navigation capability and for integrated INS/Doppler capability.

3.3 SYSTEM FUNCTIONS - The SCNS primary function is to provide highly accurate and reliable self-contained navigation capability for the MAC C-130 Tactical Airlift Operations. These missions and operations are defined in MACR 55-130, Military Airlift Command Regulation.

3.3.1 MAJOR FUNCTIONS - The SCNS provides the following major functions.

- Navigation modes and position update capability.
- Integrated control and display of navigation, communication, guidance, and steering functions.
- Aircraft guidance and steering - including flight plan, time of arrival, CARP, SAR, and rendezvous.

3.3.2 SECONDARY FUNCTIONS - Additional features are provided to improve performance, reduce crew workload, and minimize aircraft maintenance time. Specifically, these are:

- TACAN mixing to improve navigation accuracy.
- CARP capability that will reduce crew workload and increase mission flexibility.
- Simple, accurate, and quick magnetic compass calibration procedures.

3.4 A-KITS - The "A" kits will consist of:

- ☐ The interconnecting cables between added LRUs.
- ☐ The interconnecting cables and modifications to cables connecting existing LRUs.
- ☐ Mounting trays and hardware.
- ☐ Sheet metal work as required.
- ☐ Control panels
- ☐ Blank panels
- ☐ Annunciator lights
- ☐ Pressure sensors
- ☐ Circuit breaker changes and additions.

4.0 SAFETY CRITERIA - Certain safety criteria IAW MIL-STD-882A are followed in this PHA.

4.1 SYSTEM SAFETY PRECEDENCE - Any items detected as fitting into hazardous categories are treated in the following order:

a. Redesign to eliminate the hazard, if possible.

b. Change operating procedure to eliminate or reduce occurrence.

c. Provide training recommendations to allow personnel to safely work in the presence of the hazard.

d. Label or placard hazards and provide inputs to manuals.

4.2 HAZARD LEVEL CATEGORIES - (criticality definitions) For the purpose of the hazard analysis, the hazards will be defined and categorized IAW the criticality definitions set forth below (ref. MIL-STD-882A, para. 5.4.3.1).

4.2.1 HAZARD SEVERITY - Hazard severity categories are defined to provide a qualitative measure of the worst potential consequences resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, system, subsystem or component failure or malfunction as follows:

a. Category I - Catastrophic - May cause death or system loss.

b. Category II - Critical - May cause severe injury, severe occupational illness, or major system damage.

c. Category III - Marginal - May cause minor injury, minor occupational illness, or minor system damage.

d. Category IV - Negligible - Will not result in injury, occupational illness, or system damage.

4.2.2 HAZARD PROBABILITY - The probability of the defined hazard occurring is based on a qualitative judgement for the purpose of this hazard analysis. The probability levels quoted here are from MIL-STD-882A, Para. 5.4.3.2.

DESCRIPTIVE WORD	LEVEL	SPECIFIC INDIVIDUAL ITEM	FLEET OR INVENTORY
Frequent	A	Likely to occur frequently	Continuously experienced
Reasonably Probable	B	Will occur several times in life of an item	Will occur frequently
Occasional	C	Likely to occur sometime in life of an item	Will occur several times
Remote	D	So unlikely, it can be assumed that this hazard will not be experienced	Unlikely to occur but possible
Extremely Improbable	E	Probability of occurrence cannot be distinguished from zero.	So unlikely, it can be assumed that this hazard will not be experienced.
Impossible	F	Physically impossible to occur	Physically impossible to occur

4.3 HAZARD ANALYSIS MATRIX SHEETS - Due to the preliminary and limited data available at this time, the Hazard Analysis Matrix sheets reflect safety concerns. Hazards described may not exist in the final configuration. The Hazard Classes should be considered as based on concerns and estimates, and are not to be construed as reflections on the final design. Later reports (other data items) will reflect the elimination or correction of such potential hazards.

APPENDIX I

HAZARD ANALYSIS MATRIX SHEETS

SYSTEM: SCNS

SUBSET: Installation Design

PRELIMINARY HAZARD ANALYSIS

Prepared by: J.T.Reeves
Page: 1 of 5
Revision: - Rev -

ITEM NO.	OP MODE	FAILURE MODE	FAILURE EFFECT	HAZARD DESCRIPTION	CL	LV	CONTROLS AND COMMENTS
1	Flight	Water soaked	Loss of use of co-pilots ICDU	Loss of control of TACAN 2, HF 2, VOR/ILS 2, VHF 2 (may pass through control area if keyboard and display fail).	III	B	Front panel and sides of case of ICDU must be totally watertight, or window over ICDU must always be closed and leakproof when aircraft is parked. Correction will reduce level to E.
2	Flight	Switch accidentally off	No Doppler input	DVS XMIT ON/OFF switch easily knocked to OFF.	III	C	Switch needs to be guarded, pull to actuate or a rotary should have indicator light to indicate xmitting. Adequate design will reduce class to IV and level to E.

CLASS: I CATASTROPHIC
II CRITICAL
III MARGINAL
IV NEGLIGIBLE

LEVEL: A - FREQUENT
B - REASONABLY PROBABLE
C - OCCASIONAL
D - REMOTE
E - EXTREMELY IMPROBABLE
F - IMPOSSIBLE

SYSTEM: SCNS

SUBSET: Maintenance

PRELIMINARY HAZARD ANALYSIS

Prepared by: J.T.Reeves
Page: 2 of 5
Revision: - Rev -

ITEM NO.	OP MODE	FAILURE MODE	FAILURE EFFECT	HAZARD DESCRIPTION	CL	LV	CONTROLS AND COMMENTS
3	Maintenance	Superficial damage	Removal attempt of ICDU	Scratch, gouge or otherwise damage ICDU in removal attempt.	III	C	Handles are being designed for the face of the ICDU. Proper design will reduce class to IV and level to E.
4	Maintenance	N/A	N/A	Weights: DVS: 73 lbs INU: 45 lbs INU Battery: 80 lbs Personnel lifting injuries	III	B	Label each LRU with a weight placard indicating a 2 or 3 person lift requirement will reduce level to E.

CLASS: I CATASTROPHIC
II CRITICAL
III MARGINAL
IV NEGLIGIBLE

LEVEL: A - FREQUENT
B - REASONABLY PROBABLE
C - OCCASIONAL
D - REMOTE
E - EXTREMELY IMPROBABLE
F - IMPOSSIBLE

SYSTEM: SCNS

SUBSET: Flight

PRELIMINARY HAZARD ANALYSIS

Prepared by: J.T.Reeves
Page: 3 of 5
Revision: - Rev -

ITEM NO.	OP MODE	FAILURE MODE	FAILURE EFFECT	HAZARD DESCRIPTION	CL	LV	CONTROLS AND COMMENTS
5	Flight	Two altitude references.	Design item, not a failure.	Altitude confusion: SCNS receives altitude data from added pressure sensor. Pilot also has baro alt indicator. Must make separate pressure altitude correction entries.	III	A	Use of encoded altimeter as source of altimeter setting data will reduce concern to level D.
6	Flight	Jump or drop after last minute abort decision.	Design item, not a failure.	Jump light or drop light comes on automatically IAW SCNS Navigation data. Last minute abort decision due to non-navigational inputs must be made. Lights come on anyway.	IV	D	A switch currently exists at the Co-pilot station to provide manualoverride of the jump lights. Present intent is not to modify it. It will be analyzed and if found satisfactory, will not be modified.

CLASS: I CATASTROPHIC
II CRITICAL
III MARGINAL
IV NEGLIGIBLE

LEVEL: A - FREQUENT
B - REASONABLY PROBABLE
C - OCCASIONAL
D - REMOTE
E - EXTREMELY IMPROBABLE
F - IMPOSSIBLE

SYSTEM: SCNS

SUBSET: Flight/Flight Line

PRELIMINARY HAZARD ANALYSIS

Prepared by: J.T.Reeves
Page: 4 of 5
Revision: - Rev -

ITEM NO.	OP MODE	FAILURE MODE	FAILURE EFFECT	HAZARD DESCRIPTION	CL	LV	CONTROLS AND COMMENTS
7	Flight or Flight Line	Pilots ICDU fails.	Loss of X-track error. VHF #1 UHF #1 HF #1	Degrades communication and slightly degrades navigation.	III	C	Provide 2nd source of X-track data and also consider in-flight swap out of ICDU's. If swap is considered, then provisions are required to retain all required memory during power-down swap out or to provide for the safe removal and replacement with power on. Retain manual radio head with switch-over for UHF #1. Correction will reduce concern to level D.
8	Flight	Any ICDU fail.	Loss of control of those radios switched by the failed ICDU.	Radio may shut down upon loss of ICDU.	III	C	Design interface such that radio stays active on last assigned frequency unless commanded off. Loss of ICDU should not cause RCVR to go OFF or to change channels randomly. Level will reduce to F.

CLASS: I CATASTROPHIC
II CRITICAL
III MARGINAL
IV NEGLIGIBLE

LEVEL: A - FREQUENT
B - REASONABLY PROBABLE
C - OCCASIONAL
D - REMOTE
E - EXTREMELY IMPROBABLE
F - IMPOSSIBLE

SYSTEM: SCNS

SUBSET: Maintenance/Flight

PRELIMINARY HAZARD ANALYSIS

Prepared by: J.T.Reeves
Page: 5 of 5
Revision: - Rev -

ITEM NO.	OP MODE	FAILURE MODE	FAILURE EFFECT	HAZARD DESCRIPTION	CL	LV	CONTROLS AND COMMENTS
9	Ramp	None	None	Cooling fan noise excessive.	III	A	Fan type not selected yet. Low noise types will reduce this concern to class IV, level E.
10	Flight and Maintenance	Any which still allow CRT messages.	Loss of some function.	May not know extent of functional loss or types of errors introduced.	II	C	Assure that default modes have adequate annunciation or interactive cues to crew. Assure, to the extent possible, that reasonable but erroneous data contains warnings or that can be compared by crew members with other data sources. Correct design in this area will reduce the concern to class III, level D.

CLASS: I CATASTROPHIC
II CRITICAL
III MARGINAL
IV NEGLIGIBLE

LEVEL: A - FREQUENT
B - REASONABLY PROBABLE
C - OCCASIONAL
D - REMOTE
E - EXTREMELY IMPROBABLE
F - IMPOSSIBLE

END

FILMED

1-86

DTIC